

REMARKS

Claims 1-39 are pending in the present application. Claim 1 is amended to correct a typographical error that does not affect the scope of the claim. Reconsideration of the claims is respectfully requested.

Applicants thank the examiner for the interview of June 28, 2005. The rejection of claim 1 was discussed during the interview. No agreement was reached.

I. 35 U.S.C. § 103, Obviousness

The examiner rejects claims 1-39 under 35 U.S.C. § 103(a) as obvious over *Ogdon et al.*, Method and System for Providing a Presentation on a Network, U.S. Patent 6,161,137 (Dec. 12, 2000). This rejection is respectfully traversed.

The examiner states that:

4. Claims 1-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ogdon et al* (US 6,161,137).
 - a. Referring to claim 1:
 - i. *Ogdon* teaches:
 - (1) requesting the content from a source using a set of identifiers; receiving the content from the source to form received content; wherein at least one returned identifier is returned from the source in which at least one returned identifier is returned from the source in which at least one returned identifier represents a location of the content i.e., for a given presentation, the present invention directs each client node to request presentation content from a given set of communications network servers rather than having such servers push presentation content to the client node (column 6, lines 40-44). Further, each host 200 receives from the lobby system 144 audience member identifications for each presentation performance controlled by the host immediately prior to the performance of the presentation. Note that each such audience member identification typically includes: (a) a unique six digit client identifier which is encoded into the client presentation software 88 for each presentation performance client, and (b) a three digit group identifier for assigning one or more web servers 96 to provide presentation content (column 11, lines 64-67 through column 12, lines 1-5). In addition, resources may be allocated for a presentation according to the number and geographical locations of clients desiring to

participate in a particular presentation (column 12, lines 27-29);

(3) sending identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the content at the source; and responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, selectively preventing receipt of additional content from the source i.e., For each presentation performance, the presentation controlling host 200 also receives, from a presentation performance specific resource file or data base 212: (a) content webserver 96 network addresses (e.g., for the Internet, these addresses being URLs) identifying the network 70 sites having presentation content data; (b) audience member lists of clients that have registered for the presentation performance and can therefore become audience members, if they choose to; (c) groupings of registered clients; and (d) script names and locations from which to retrieve the presentation script from the content manager 104. Accordingly, note that the records of the corresponding resource file 212 associate presentation identifiers with content webserver 96 URLs and path names on these webserver where presentation content data resides. Thus, since the presentation scripts received by the hosts 200 from the content manager 104 are generic in that the scripts have variables or placeholders for content webserver 96 identities, each host 200 uses information from the corresponding resource file 212 (retrieved according to presentation identification) for resolving the undefined content webserver variables of the generic scripts, and thereby instantiating presentation scripts and presentation data with specific content webserver 96 references. Note that the resource file 212 may be created from information in a scheduling data base (not shown) populated with, e.g., content webserver 96 groupings (each grouping for supplying presentation content to a particular group of audience members) and audience member group identifications. The grouping of the webserver and the audience member groupings are both indicated by the three digit group identifier also encoded into each copy of the client presentation software 88 distributed by the software download and client support system 130 as previously discussed (column 12, lines 30-62).

ii. Although *Ogdon* does not explicitly mention selectively preventing receipt of additional and/or duplicate content from the source, *Ogdon* does imply that:

(1) the content manager 104 distributes presentation content (e.g., presentation segments) to the content webserver 96 and verifies that the content is capable of being presented to audience members immediately before a presentation time. Note that the verification process makes sure that all the links in the presentation or show can be resolved appropriately. Finally, at the end of a presentation performance, the content manager 104 may remove the presentation content from one or more of the content webserver 96 (column 9, lines 44-53).

(iii) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly discuss or point out the role of the content manager system 104 as in *Ogdon* for distributing presentation data and/or content and to make sure there is no duplication or extra presentation data (column 9, lines 27-53).

(iv) The ordinary skilled person would have been motivated to:

(1) clearly discuss or point out the role of the content manager system 104 as in *Ogdon* for distributing presentation data and/or content in order to maintain the cost of the material and to prevent unauthorized members from using/accessing the content.

Office Action of April 19, 2005, pp. 2-4 (emphasis in original).

If the Patent Office does not produce a *prima facie* case of unpatentability, then without more, the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). A *prima facie* case of obviousness is established when the teachings of the prior art itself suggest the claimed subject matter to a person of ordinary skill in the art. *In re Bell*, 991 F.2d 781, 783, 26 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1993). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). A proper *prima facie* case of obviousness cannot be established by combining the teachings of the prior art absent some teaching, incentive, or suggestion supporting the combination. *In re Napier*, 55 F.3d 610, 613, 34 U.S.P.Q.2d 1782, 1784 (Fed. Cir. 1995); *In re Bond*, 910 F.2d 831, 834, 15 U.S.P.Q.2d 1566, 1568 (Fed. Cir. 1990).

Amended claim 1 is as follows:

1. A method in a data processing system for detecting monitoring of access to content, the method comprising the data processing system implemented steps of:
 - requesting the content from a source using a set of identifiers;
 - receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content;
 - sending identifiers to a validation service, wherein the identifiers include the set of identifiers used to request the received content and each returned identifier representing the location of the content at the source; and
 - responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, selectively preventing receipt of additional content from the source.

A. The Examiner Has Failed To State A *Prima facie* Obviousness Rejection Against Claim 1

The examiner has failed to state a *prima facie* obviousness rejection against claim 1 for the following reasons. First, not all of the claimed features are shown or suggested by *Ogdon*. Second, the examiner has failed to provide a proper motivation to modify the reference. Third, the reference is not analogous art because the reference is in a different field and not pertinent to the present invention.

1. All of the Claim Features Are Not Present in or Suggested by *Ogdon*

The examiner has failed to state a *prima facie* obviousness rejection because the features that the examiner states as being present in *Ogdon* are not found or suggested in *Ogdon*. In particular, *Ogdon* does not show or suggest the claimed features of (a) receiving content and at least one returned identifier, (b) sending the set of identifiers used to request the received content and each returned identifier to a validation service, or (c) responsive to the validation service indicating monitoring of user requests to access content is occurring, selectively preventing receipt of additional content from the source.

The examiner asserts that *Ogdon* does show these features, citing the following portions of *Ogdon*:

For a given presentation, the present invention directs each client node to request presentation content from a given set of communications network servers rather than having such servers push presentation content to the client node.

...

(4.6) Content Manager 104: A content manager system 104 for managing presentation scripts and data. The content manager 104 logs and confirms the locations and addresses of content webserver 96 where the content for each presentation will reside. The content manager 104 distributes presentation data, such as scripting information for a presentation, thereby providing:

(a) initial groupings of audience members according to, e.g., natural language preferred, organizational affiliation, geographical location, and/or intervening network connections and devices (e.g., firewalls and other security features, local area network connections), and/or

(b) sequencing of presentation segments to the operations center 58 (and more particularly, the host(s) 200 described hereinbelow).

Additionally, the content manager 104 distributes presentation content (e.g., presentation segments) to the content webserver 96 and verifies that the content is capable of being presented to audience members immediately before a presentation time. Note that the verification process makes sure that all the links in the presentation or show can be resolved appropriately. Finally, at the end of a presentation performance, the content manager 104 may remove the presentation content from one or more of the content webserver 96.

Further note that the content manager 104 includes a reservation system 108 for maintaining a schedule for presentation and for reserving resources of the operations center 58, and any presentation leader support such as leader stations 92. The content manager 104 also includes an invitation subsystem 112 that is capable of maintaining invitation lists of candidate audience members, together with corresponding addresses (e.g., e-mail addresses) for various presentation performances. Additionally, the invitation subsystem 112 is capable of accessing client profile information for past audience members residing in the profile database 120. Accordingly, by comparing client profile information in the profile database 120 with the information in

various invitation lists, and/or presentation descriptions (e.g., keywords, etc.), prospective audience members for a particular presentation can be notified of future similar presentations via, e.g., e-mail.

...

Additionally, the content manager 104 distributes presentation content (e.g., presentation segments) to the content webserver 96 and verifies that the content is capable of being presented to audience members immediately before a presentation time. Note that the verification process makes sure that all the links in the presentation or show can be resolved appropriately. Finally, at the end of a presentation performance, the content manager 104 may remove the presentation content from one or more of the content webserver 96.

...

Further, each host 200 receives from the lobby system 144 audience member identifications for each presentation performance controlled by the host immediately prior to the performance of the presentation. Note that each such audience member identification typically includes: (a) a unique six digit client identifier which is encoded into the client presentation software 88 for each presentation performance client, and (b) a three digit group identifier for assigning one or more webserver 96 to provide presentation content.

...

In addition, resources may be allocated for a presentation according to the number and geographical locations of clients desiring to participate in a particular presentation.

...

For each presentation performance, the presentation controlling host 200 also receives, from a presentation performance specific resource file or data base 212: (a) content webserver 96 network addresses (e.g., for the Internet, these addresses being URLs) identifying the network 70 sites having presentation content data; (b) audience member lists of clients that have registered for the presentation performance and can therefore become audience members, if they choose to; (c) groupings of registered clients; and (d) script names and locations from which to retrieve the presentation script from the content manager 104. Accordingly, note that the records of the corresponding resource file 212 associate presentation identifiers with content webserver 96 URLs and path names on these webserver 96 where presentation content data resides. Thus, since the presentation scripts received by the hosts 200 from the content manager 104 are generic in that the scripts have variables or placeholders for content webserver 96 identities, each host 200 uses information from the corresponding

resource file 212 (retrieved according to presentation identification) for resolving the undefined content webserver variables of the generic scripts, and thereby instantiating presentation scripts and presentation data with specific content webserver 96 references. Note that the resource file 212 may be created from information in a scheduling data base (not shown) populated with, e.g., content webserver 96 groupings (each grouping for supplying presentation content to a particular group of audience members) and audience member group identifications. The grouping of the webserver and the audience member groupings are both indicated by the three digit group identifier also encoded into each copy of the client presentation software 88 distributed by the software download and client support system 130 as previously discussed.

Ogdon, col. 6, ll. 40-44; col. 9, ll. 44-53; col. 9, ll. 27-53; col. 11, ll. 64-67 through col. 12, ll. 1-5; col. 12, ll. 27-29; and col. 12, ll. 30-62.

However, contrary to the examiner's assertions, these portions of *Ogdon* do not show or suggest receiving content *and* at least one returned identifier. In claim 1, the returned identifier is not part of the set of identifiers used to access the content. The above portions of *Ogdon* teach using an audience member identifier to initially access presentation content. *Ogdon* does not show or suggest receiving at least one returned identifier in addition to receiving content. Thus, *Ogdon* does not show or suggest all of the features as suggested by the examiner. Accordingly, the examiner has failed to state a *prima facie* obviousness rejection of claim 1.

Regarding the feature of sending the set of identifiers used to request the received content and each returned identifier to a validation service, the examiner asserts that *Ogdon* does show this feature, citing column 12, lines 30-62 of *Ogdon*, which is quoted above. However, contrary to the examiner's assertions, this portion of *Ogdon* does not show or suggest sending the set of identifiers used to request the received content *and* each returned identifier to a validation service because *Ogdon* makes no mention of a returned identifier. *Ogdon* teaches providing registered clients a presentation identifier and validating the presentation identifier before allowing clients access. *Ogdon* does not show or suggest sending the identifiers used to request content and each returned identifier to a validation service after receiving content. Thus, *Ogdon* does not show or suggest all of the features of claim 1. Accordingly, the examiner has failed to state a *prima facie* obviousness rejection of claim 1.

Regarding the feature of validation, *Ogdon* uses a validation server and the present invention uses a validation service. Merely because both *Ogdon* and claim 1 use the word 'validation' does not mean that both are the same. The validation service in claim 1 is provided with different parameters, has a different purpose, and is used in a different context than *Ogdon's* validation server, as described in detail below.

More specifically, in *Ogdon*, the content provider validates the audience member's identifier before allowing the audience member access to content. In contrast, in the present invention, the user accesses a content provider and receives content, and then a validation service is used to detect whether the content provider is monitoring user requests to access content.

In *Ogdon*, validation is described as follows:

In step 416, the pre-show control system 136 accepts network 70 and/or network 74 connections by candidate clients for the presentation performance. Note that it is assumed that the clients have previously registered for the presentation performance with the registration module 140 and therefore have been provided with validation information (e.g. a presentation performance identifier and/or password) for validating each client as an audience member for the presentation. Subsequently, in step 420, a determination is made by the pre-show control system 136 as to whether each candidate presentation audience member is connected to the pre-show control system by the communications network 70 or by the telephony network 74. If it is determined that a candidate presentation client is connected by the communications network 70, then step 424 is performed, wherein the candidate client logs onto the pre-show control 136 with a previously provided login. Note that this login may include a presentation performance identifier for the presentation and a password for identifying the candidate client as being registered for the presentation performance. Further note that in one embodiment, this step is performed by the lobby system 144. Subsequently, in step 428, a determination is made by the pre-show control system 136 (or the lobby system 144) as to whether the entered login is valid. If the login is determined to be invalid, then step 432 is performed wherein the connection with the pre-show control system 136 is terminated. Note however, it is within the scope of the present invention that various retries can be provided as one skilled in the art will understand. Alternatively, if the candidate client's login is determined to be valid, then step 436 is performed wherein the pre-show control (determines whether the client's client node 56 is configured appropriately for the presentation performance). In

particular, the pre-show control system 136 determines whether the client presentation software 88 is operable on the client's client node 56. Further, the pre-show control system 136 may also determine whether the client's client node 56 has the appropriate network 70 addresses (e.g. URLs) of the content webserver 96 available for supplying presentation segments to the client node.

Ogdon, col. 18, l. 57 through col. 19, l. 29.

In summary, a client first registers to view a presentation performance and is provided a presentation identifier. Next, on the date and time the presentation performance is given, the client supplies the presentation identifier, and the validation server determines whether the presentation identifier is valid or not. If the validation server determines that the client's presentation identifier is valid, the client is then allowed to access presentation content. But, if the identifier is not valid, the connection is terminated and the client is not allowed to access *any* presentation content. Thus, the validation server is provided and asked to validate a presentation identifier *before* the client is allowed access to any content, and if the identifier is not valid, the termination of the connection prevents the client from accessing any presentation content.

In contrast, in claim 1, a user requests access to content using a set of identifiers and receives content and returned identifiers. Claim 1 also recites that the validation service is then provided (i) the identifiers used to receive the content and (ii) the returned identifiers to determine whether user requests to access content is being monitored. If the validation service determines monitoring of user requests to access content is occurring, then the user is selectively prevented from receiving additional content from that source. Thus, in claim 1, the validation service is provided the set of identifiers used to access the content and the returned identifiers, *after* the user receives content.

Because *Ogdon*'s validation server validates whether a client is authorized to access a presentation, only the presentation identifier is provided to the validation server for validation. *Ogdon* does not provide the returned identifiers to the validation server. In contrast, in claim 1, the validation service is provided (1) the identifiers used to access the content and (2) the returned identifiers.

Thus, *Ogdon*'s validation server validates the presentation identifier *before* a client can access any presentation content to prevent unauthorized clients from accessing presentations. In contrast, the present invention allows a user to receive content and

returned identifiers, and *afterwards* validates whether monitoring of user requests to access content are occurring. The present invention's validation service validates different parameters, occurs in a different context (after rather than before receiving content), and serves a different purpose. Nothing in *Ogdon* suggests otherwise. Thus, the reference does not show or suggest all the features of claim 1 as asserted by the examiner. Accordingly, the examiner has failed to state a *prima facie* case of obviousness.

Regarding the feature of selectively preventing receipt of additional content from the source, the examiner acknowledges that *Ogdon* does not show this feature. Office Action of April 19, 2005, p. 4. The examiner goes on to assert that *Ogdon* implies this feature, citing the following portions of *Ogdon*:

Content manager 104 distributes presentation content (e.g., presentation segments) to the content webserver 96 and verifies that the content is capable of being presented to audience members immediately before a presentation time. Note that the verification process makes sure that all the links in the presentation or show can be resolved appropriately. Finally, at the end of a presentation performance, the content manager 104 may remove the presentation content from one or more of the content webserver 96.

Ogdon, col. 9, ll. 44-53.

However, contrary to the examiner's assertions, the cited portion of *Ogdon* does not show or suggest selectively preventing receipt of *additional* content from the source. *Ogdon* teaches removing presentation content at the end of a presentation after the client has accessed the content. *Ogdon* also teaches preventing unauthorized clients from accessing presentation content. *Ogdon* does not teach a user accessing and receiving content, detecting whether the user's requests to access content are being monitored, and then preventing receipt of additional content if the user's requests are being monitored.

In *Ogdon*, clients with valid presentation identifiers can access content while clients with invalid presentation identifiers do not get access to any content. Thus, in *Ogdon*, access to content is determined by the validity of the presentation identifier. In contrast, in claim 1, after the user initially receives content and a set of returned identifiers, if the validation service detects monitoring of user requests to access content is occurring, then the user is selectively prevented from receiving *additional* content. Thus, in the present invention, access to content is not determined by the validity of the

presentation identifier. Unlike *Ogdon*, in claim 1 access to content is determined by whether or not the content provider is monitoring user requests to access content. Thus, the proposed interpretations of the cited reference are incorrect. Accordingly, the examiner has failed to state a *prima facie* obviousness rejection of claim 1.

In summary, *Ogdon* does not show or suggest the claimed features of receiving content and at least one returned identifier, sending the identifiers used to request the content and each returned identifier to a validation service, or selectively preventing receipt of additional content from the source responsive to the validation service indicating monitoring of user requests to access content is occurring. Therefore, the examiner has failed to state a *prima facie* obviousness rejection.

2. The Examiner Has Failed to State Proper Motivation to Modify the Reference

The examiner has failed to state a *prima facie* obviousness rejection because the examiner has failed to state a proper motivation to modify *Ogdon*. The examiner states that an "ordinary skilled person would have been motivated to... prevent unauthorized members from using/accessing the content". Office Action of April 19, 2005, p. 4. However, this statement does not state any motivation to modify the reference to detect monitoring of user's requests to access content. The cited reference discusses monitoring client requests to access presentation content but there is no motivation in the reference to detect when monitoring of requests occurs. Because the examiner must state a proper motivation to modify the reference, the examiner has failed to state a *prima facie* obviousness rejection.

Similarly, the examiner has provided no support for the proposition that allowing registered clients access to a presentation on a network using a presentation identifier and detecting monitoring of user requests to access content are in any way equivalent. Thus, the examiner's statement is logically insufficient to establish that one feature may be substituted for another or that a motivation exists to modify *Ogden*. Accordingly, again, the examiner has failed to state a *prima facie* obviousness rejection.

The examiner has also failed to state any motivation as to why detecting when a content site is monitoring user requests to access content would be obvious in view of

Ogdon. *Ogdon* makes a presentation available to clients on a network, so *Ogdon* teaches validating a presentation identifier to determine whether a client is authorized to access the presentation. However, there is no motive to validate whether monitoring of user access to content is occurring because in *Ogdon*, once the user has access to the content, validation has already been performed. The examiner has thus failed to state a proper motivation to modify *Ogdon* to achieve these claimed features. The examiner has accordingly failed to state a *prima facie* obviousness rejection.

In addition, the examiner's statement does not serve as a proper motivation to modify *Ogdon* because the statement makes no sense vis-à-vis *Ogdon* and claim 1. Claim 1 provides for selectively preventing receipt of content responsive to a response from a validation service indicating that monitoring of user requests to access the received content is occurring. The examiner's statement refers to selectively blocking unauthorized users, while the claimed method requires preventing receipt of content if monitoring is occurring. Thus, if the examiner's statement were used to modify *Ogdon*, then all users would be prevented from receiving content as soon as the content provider started monitoring. This result would be contrary to *Ogdon*'s purpose of making a presentation available to users, and so the examiner's statement cannot be construed as motivation to modify *Ogdon*. Accordingly, the examiner has failed to state a *prima facie* case of obviousness.

3. *Ogdon* is Non-Analogous Art

The examiner has failed to state a *prima facie* obviousness rejection because *Ogdon* is non-analogous art and therefore the examiner may not use *Ogdon* as a reference. "In order to rely on a reference as a basis for rejection of the applicant's invention, the reference must either be in the field of the applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." *In re Oetiker*, 977 F.2d 1443, 1447 (Fed. Cir. 1992).

Ogdon is in the field of providing a presentation on a network. *Ogdon*, col. 1, ll. 1-2. On the other hand, the claimed invention is in the field of identifying rewriting of universal resource locators in content requested by a user. Specification, p. 1, ll. 13-14.

These two fields are different from each other. Because the fields are distinct, *Ogdon* fails the first test of *Oetiker*.

In addition, *Ogdon* is not reasonably pertinent to the particular problem solved by the present invention. *Ogdon* pertains to the problem of delivering a presentation to users with differing network characteristics. *Ogdon*, col. 1, ll. 9-15. In contrast, the claimed invention pertains to the problem of ensuring a user's privacy when a website is monitoring user behavior. Specification, p. 3, ll. 22-25; claim 1. These two problems have nothing to do with each other and so *Ogdon* is not reasonably pertinent to the problem to be solved. Hence, *Ogdon* also fails the second test of *Oetiker*.

Moreover, In *In re Oetiker*, the Court held "it has not been shown that a person of ordinary skill, seeking to solve a problem of fastening a hose clamp, would reasonably be expected or motivated to look to fasteners for garments." *Id.* The Court found that even though fasteners for hose clamps are similar to fasteners for garments, the latter is non-analogous art to the former. *Id.* In the case at hand, *Ogdon* is completely dissimilar to the invention of claim 1, for the reasons presented above. Given that the claimed invention is much more dissimilar to *Ogdon* than fasteners for garments are dissimilar to fasteners for hose clamps; *Ogdon* is non-analogous art to claim 1 under the standards of *In re Oetiker*.

Because *Ogdon* fails both tests of *In re Oetiker*, *Ogdon* is non-analogous art. The examiner may therefore not use *Ogdon* as a reference when stating an obviousness rejection against claim 1. Accordingly, the examiner has failed to state a *prima facie* obviousness rejection of claim 1.

B. The Claims Are Not Obvious in View of *Ogdon*

1. The Reference Addresses a Different Problem

Ogdon and the present invention are in different fields and address different problems. As previously shown, *Ogdon* is concerned with providing a presentation over a network and ensuring only authorized users access the presentation. *Ogdon* addresses the problem of how to make a presentation available to participants with differing network characteristics. In contrast, claim 1 addresses the problem of ensuring user privacy. The present invention detects when a content provider is monitoring user

requests to access content, and prevents receipt of further content if monitoring is detected. One skilled in the art would have no motivation to modify *Ogdon* to address the problem of validating whether user requests to access content are being monitored. Accordingly, claim 1 is not obvious in view of *Ogdon*.

2. Claim 1 Solves an Unrecognized Problem

Furthermore, claim 1 is non-obvious because claim 1 solves a problem unrecognized by *Ogdon*. Claim 1 solves the problem of detecting when a content-provider is monitoring user requests to access content. *Ogdon* does not provide any indication that the inventor was even aware of this problem. As previously shown, in *Ogdon*, both the user and validation server are aware that the presentation content provider is monitoring user access to content and so there is no need to detect whether user requests are being monitored. In contrast, in the present invention, the user and validation server are unsure whether the content provider is monitoring user access to content and so there is a need to detect when monitoring is occurring. Because claim 1 solves a problem that *Ogdon* does not recognize, claim 1 is non-obvious in view of *Ogdon*.

3. The Proposed Modification Would Result in an Unworkable Method

Furthermore, it would not be obvious to allow unauthorized users access to content prior to validating the content identifier used to access the content because doing so would defeat the purpose of validating presentation identifiers. In *Ogdon*, the validation server validates the user's presentation identifier, and if the identifier is valid, the user is allowed access to content. If the identifier is invalid, the user is not allowed access to content. *Ogdon*, column 19, lines 13-23. In contrast, in claim 1, users first access and receive content and then afterwards the validation service validates whether monitoring of user requests to access content is occurring. Furthermore, in claim 1, receipt of additional content is prevented if monitoring is detected.

If *Ogdon*'s teaching were used to modify claim 1 as suggested by the examiner, then no one would gain access to content. As users attempt to access content in the system of the proposed modification, the validation server in *Ogdon* would detect that

users were accessing content. This seems to be the basis for the examiner's apparent belief that monitoring of access to content inherently occurs in *Ogdon*. However, claim 1 provides that if monitoring of access to content is detected, then receipt of additional content is selectively prevented. Thus, the instant that a user attempted to gain access to content, the validation server of the proposed modification would detect the access to the content, monitor the access to the content, detect that monitoring has occurred, and, as a result, subsequently block additional receipt of content. Accordingly, the user would never receive content if the examiner's proposed modification were implemented. Permanently blocking access to content defeats the purpose of *Ogdon*, which is to provide content to users. Furthermore, permanently blocking access to content in this manner serves no useful function. Accordingly, the proposed modification would be unworkable. Therefore, there is no motivation to modify the present invention and for this reason claim 1 is non-obvious.

C. Summary of Why Claim 1 Is Allowable Over *Ogdon*

The examiner has failed to state a *prima facie* case of obviousness against claim 1 because (i) features that the examiner states as being present in *Ogdon* are not found or suggested in *Ogdon*, (ii) the examiner has failed to state proper motivation to modify the reference, and (iii) *Ogdon* is non-analogous art. Additionally, the claim 1 is not obvious in view of *Ogdon* because *Ogdon* addresses a different problem than that addressed by claim 1, because claim 1 solves a problem unrecognized by *Ogdon*, and because the proposed modification would result in an unworkable method. Therefore, the rejection of claim 1 under 35 U.S.C. § 103 has been overcome.

D. Remaining Claims

Independent claims 8, 16, 19, 21, 22, 29, 37, and 38, contain limitations similar to those presented in claim 1. Therefore, the examiner has failed to state a *prima facie* obviousness rejection of these claims for the reasons presented above. Similarly, these claims are non-obvious in view of *Ogdon* for the reasons presented above.

The remaining dependent claims depend from claims 1, 8, 16, 19, 21, 22, 29, 37, and 38 accordingly. Therefore, these claims should be allowable over *Ogdon* at least for

the reasons presented above. In addition, these claims contain other features not shown or suggested by *Ogdon*. For example, *Ogdon* does not show or suggest identification of the source in a service used to prevent receipt of content from identified sources as claimed in claim 6. Thus, the remaining dependent claims should also be allowable over *Ogdon*.

The examiner has failed to state a *prima facie* obviousness rejection of any of the claims. In addition, all of the claims are non-obvious over *Ogdon*. Therefore, the rejection under 35 U.S.C. § 103(a) has been overcome.

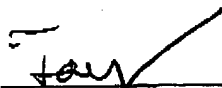
II. Conclusion

It is respectfully urged that the subject application is patentable over *Ogdon* and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: July 14, 2005

Respectfully submitted,



Theodore D. Fay III
Reg. No. 48,504
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicant

TF/sn